Automated Data Processing for Public Trust Positions

2008 Data Protection Seminar
TMA Privacy Office

Purpose

- Provide an overview of Automated Data Processing (ADP) for public trust positions and the role of the TRICARE Management Activity (TMA) Privacy Office as it pertains to contractor personnel

Objectives

- This presentation will:
  - Explain TMA Privacy Office's role in ADP for public trust positions
  - Clarify current policies and procedures for TMA
  - Identify common misconceptions regarding background investigations

Mission and Objective

- Mission:
  - Ensure that contractors with access to Protected Health Information/Personally Identifiable Information (PHI/PII) on Department of Defense (DoD) Information Technology (IT) Systems uphold policies and procedures against inappropriate use and disclosure of sensitive information
- Objective:
  - Provide guidance and consultation to ensure that all TMA contractor employees with access to DoD IT Systems are:
    - Trustworthy
    - Reliable
    - Of unquestionable allegiance to the United States

Automated Data Processing for Public Trust Positions

What is Personnel Security?

- The practices, technologies, and/or services used to ensure that Personnel Security safeguards are applied specifically to:
  - Contractors on TRICARE contracts
  - DoD IT systems and interconnected company owned company operated systems
  - Background investigations and trustworthiness determination
  - Granting or withdrawing system access privileges: Common Access Card (CAC)
    - Misconception
  - TMA Privacy Office Personnel Security pertains to military and government civilian personnel

Automated Data Processing for Public Trust Positions

Why Personnel Security?

- Consider the purpose of Personnel Security safeguards
  - The most common perpetrators of significant computer crimes are those with legitimate access
    - Knowingly
    - Unknowingly
  - Managing personnel with privileged access is critical
    - Recertification
      - (ADP-I, 5yrs; ADP-II, 10 yrs)
    - Change in level access

Automated Data Processing for Public Trust Positions

ADP Determination Levels

- Applicable levels of trustworthiness determinations for public trust positions:
  - **ADP/IT-I** – Critical Sensitive Position
  - **ADP/IT-II** – Non-critical Sensitive Position
- ADP/IT-IIIs are no longer authorized access to DoD IT systems
- ADP is the language formerly used for information technology positions

Automated Data Processing for Public Trust Positions

Trust Versus Security Clearances

- Positions of Trust – Individuals submit the standard Form (SF) 85 in hard copy paper only
- SF85P – Questionnaire for Public Trust Position and the FD 258 (fingerprint card) are provided to the contractor employee for completion
- Facility Security Officer (FSO) completes the Agency Use Only section of page 1 of the SF85P
- FSO prepares a cover sheet containing employee names, Social Security Number (SSN), date of birth, ADP level, and submission date of new submittals

Trust vs. Security Clearances
(continued)

- The FSO sends the cover letter and page 1 of the SF85P to the Contracting Office Representative (COR) for signature
- The COR will review, complete, and sign block “P” of the SF85P
- An asterisk (*) should be noted under the COR’s signature to denote the presence of “inquiry contact information”
- The COR reviews and  cover letter

Trust vs. Security Clearances
(continued)

- The COR will scan the cover letter and forward the document via encrypted electronic mail.
- The TMA Privacy Office (TMA PO) maintains a spreadsheet of all new submittals and checks the Joint Personnel Adjudication System (JPAS) for investigation schedule dates
- The COR returns both signed documents to the FSO, who adds his or her name and phone number to the bottom of first page of the SF85P (below block E)

Trust vs. Security Clearances
(continued)

- The FSO will send the entire SF85P and the FD258 fingerprint cards to the Office of Personnel Management (OPM)
- When OPM receives, screens, and accepts the SF85P, OPM schedules the background investigation
- OPM posts the investigation level and schedule date into the JPAS within seven to ten business days
- Rejected SF85Ps are returned to the TMA PO as Unacceptable Case Notices and forwarded to the company FSO for correction and return to OPM

Trust vs. Security Clearances
(continued)

- The TMA PO checks JPAS for the schedule date of the investigation
- Once the investigation is posted in JPAS, the TMA PO will print a copy of the JPAS printout
- The JPAS printout information is entered into the MHS database and a copy is kept in the files

Trust vs. Security Clearances
(continued)

- A copy of the JPAS printout is sent to the company FSO or designated official to notify them the investigation has been scheduled
- Interim access to DoD IT systems is allowed upon receipt of the JPAS printout
- Misconception:

  Interim access is granted upon submission of the SF85P

Automated Data Processing for Public Trust Positions

SF-86 Security Clearance

- Submitted electronically via eQIP to Defense Industrial Security Clearance Office (DISCO)
- Interim secret security clearance granted normally within 24 - 48 hours
- Fingerprints must still be mailed to OPM
- OPM schedules National Agency Check with Local Law and Credit Check (NACLC) investigation within 30 days
- Schedule date is posted in JPAS

Automated Data Processing for Public Trust Positions

Common Access Card Process

- FSO prepares the Application for DoD Common Access Card DEERS Enrollment (DD1172) and sends it to the TMA Privacy Office
- TMA Privacy Office verifies background investigation type
  - NACLC required
- DD1172 is sent to TMA Trusted Agent (TA), located in the TMA Administration Directorate
- TMA TA provides logon ID and password to the company FSO to have personnel complete the Contracting Verification System (CVS) application online

Common Access Card Process
(continued)

- TMA TA reviews and approves or rejects the CVS online application
- TA notifies the company FSO to have the employee proceed to the nearest RAPIDS location for issuance of a CAC
- Misconception:

  Everyone that submits an SF85P receives a CAC

Application Requirement: ADP/IT-I

- A written request for approval must be submitted to the TMA Privacy Officer **prior** to submitting the application to OPM
- The Letter of Request must include:
  - Thorough job description which justifies the need for the ADP/IT-I Trustworthiness Determination
  - Contact information for the Security Officer or other appropriate executive
  - Signature, at a minimum, by the company Security Officer or other appropriate executive

Automated Data Processing for Public Trust Positions

HA/TMA Network Access

- New TRICARE contractor employees who are U.S. citizens and require access to the HA/TMA Network must complete a Contractor Add User to HA/TMA Network form
- The Add User Form must be signed by the new user, company FSO, and the government program manager
- The form will then be submitted to the TMA Privacy Office for verification of appropriate ADP level

HA/TMA Network Access (continued)

- The Add User form must be approved and signed by the TMA Privacy Officer and faxed to the HA/TMA Helpdesk for processing
- The HA/TMA Helpdesk will set up the email account for the new employee pending receipt of the CAC
- When the new employee receives his or her CAC, he or she reports to the HA/TMA Helpdesk to activate the email account

Interim Access

- New TRICARE contractor employees who are U.S. citizens may be granted interim access upon receipt of the JPAS printout of the scheduled investigation by OPM

- Misconception:

  Prior language implied access granted after submission of the SF 85P and fingerprint cards to the OPM

Non-United States Citizen Access

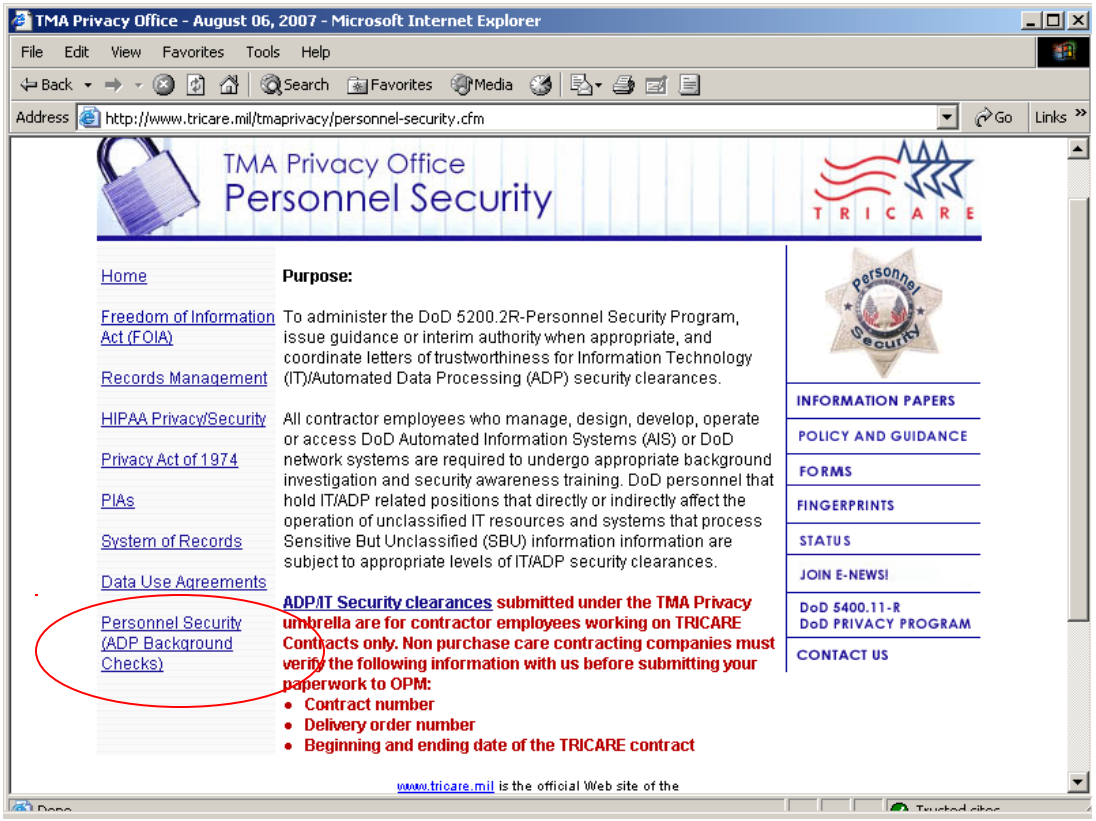
- Non-United State Citizens will **not be adjudicated** for any trustworthiness position by any government agency for TRICARE contracts
- SF85Ps will not be submitted for Non-United States citizen contractor employees

Open Issues

- Communication between contracting companies and TMA Privacy Office (e.g., New Submittals, Denial Acknowledgement, and Termination Notification)
- Sharing billing and accounting data can constitute fraud against the government
- Procedures for obtaining CAC and access to HA/TMA Network

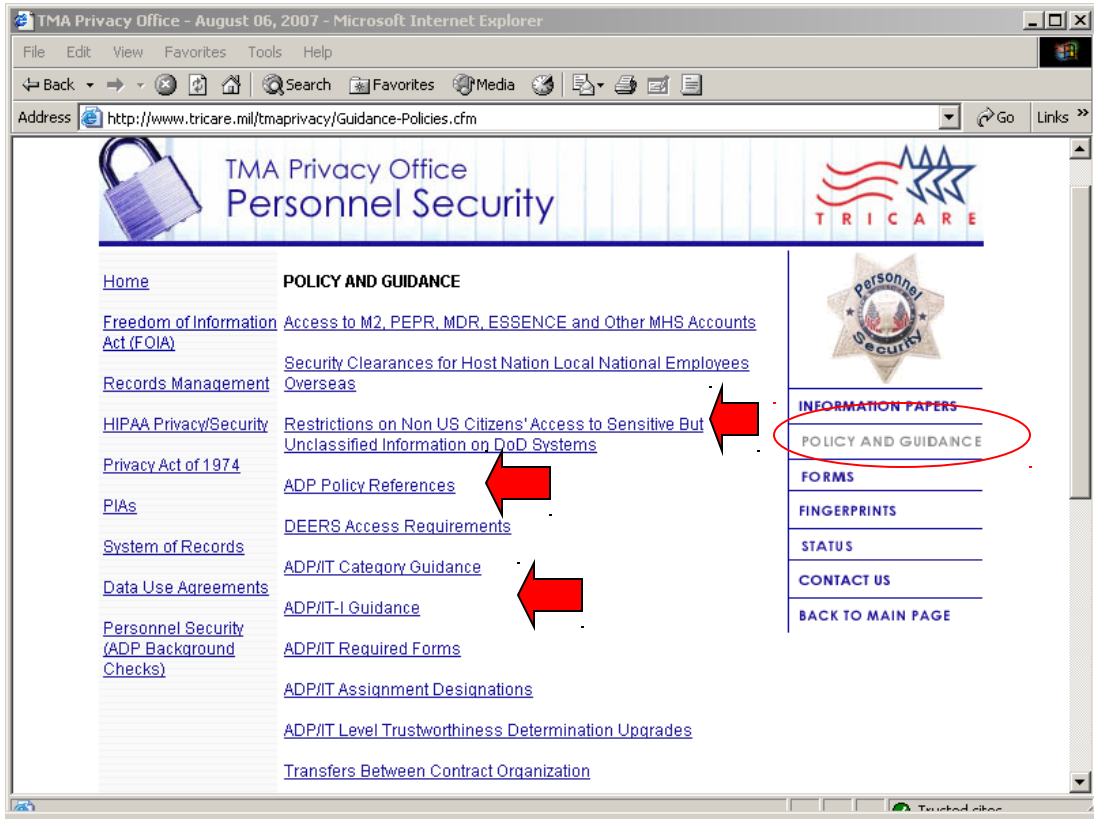
Automated Data Processing for Public Trust Positions

TMA Privacy Office Website



Automated Data Processing for Public Trust Positions

TMA Privacy Office Website (continued)



Summary

- You now can:
  - Understand TMA Privacy Office's role in Personnel Security
  - Identify current policies and procedures for TMA Personnel Security
  - Explain common misconceptions with respect to Personnel Security background investigations